(c) What win rates for AI players corresponded to an adequate level of challenge for human players?
(d) Entanglion is a play on what word?

## 4.2 States and Measurement

### *4.2.1 Tensor Product*

When we have multiple qubits, we write their states as a *tensor product* $\otimes$. For example, two qubits, both in the $|0\rangle$ state, are written

$$|0\rangle \otimes |0\rangle,$$

and this is pronounced "zero tensor zero." Often, we compress the notation and leave out the tensor product in both writing and speech:

$$|0\rangle|0\rangle.$$

We frequently compress the notation further still:

$$|00\rangle.$$

With two qubits, the $Z$-basis is $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. A general state is a superposition of these basis states:

$$c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle.$$

If we measure these two qubits in the $Z$-basis, we get $|00\rangle$ with probability $|c_0|^2$, $|01\rangle$ with probability $|c_1|^2$, $|10\rangle$ with probability $|c_2|^2$, or $|11\rangle$ with probability $|c_3|^2$. Thus, the total probability is $|c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2$, and it should equal 1.

With three qubits, there are eight $Z$-basis states $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, and $|111\rangle$. Sometimes, these binary strings are written as decimal numbers $|0\rangle, |1\rangle, \ldots, |7\rangle$. Inspired by this, let us call the right qubit the zeroth qubit, the middle qubit the first qubit, and the left qubit the second qubit, so a $Z$-basis state takes the form

$$|b_2 b_1 b_0\rangle.$$

Then, the decimal representation of this is

$$2^2 b_2 + 2^1 b_1 + 2^0 b_0.$$

In other words, we label qubits right-to-left, starting with zero. This convention, where the rightmost qubit is the zeroth qubit, is called *little endian*. Quirk and many quantum programming languages, including those in Chapter 5, also use little endian. In contrast, the opposite convention, where the leftmost qubit is the zeroth

qubit, is called *big endian*. Of note, Nielsen and Chuang's standard advanced textbook uses the big endian convention. Disputes over which convention is "better" has raged classical computing for decades, and the same debates carry into quantum computing. The reality is that you should be able to use both, but for consistency, we use little endian throughout this textbook. Next, the general state of three qubits is a superposition of these basis vectors:

$$\sum_{j=0}^{7} c_j|j\rangle = c_0|0\rangle + c_1|1\rangle + \cdots + c_7|7\rangle,$$

and the probability of getting $|j\rangle$ when measuring in the $Z$-basis is $|c_j|^2$, so $\sum_j |c_j|^2 = 1$.

With $n$ qubits, there are $N = 2^n$ $Z$-basis states, which we can label as $n$-bit strings or by the decimal numbers 0 through $N-1$. As an $n$-bit string,

$$|b_{N-1}\ldots b_1 b_0\rangle = \left|2^{N-1}b_{N-1} + \cdots + 2^1 b_1 + 2^0 b_0\right\rangle.$$

Of course, the general state of $n$-qubits is a superposition of these $Z$-basis states:

$$\sum_{j=0}^{N-1} c_j|j\rangle = c_0|0\rangle + c_1|1\rangle + \cdots + c_{N-1}|N-1\rangle.$$

This has $N$ amplitudes $c_0$ through $c_{N-1}$. Thus, if we have just $n = 300$ qubits, then we must keep track of $N = 2^{300} \approx 2.04 \times 10^{90}$ amplitudes, which is more than the number of atoms in the visible universe ($10^{78}$ to $10^{82}$). This is evidence, but not a proof, that it is difficult for classical computers to simulate quantum computers. It is evidence because classical computers cannot keep track of this many amplitudes, but it is not a proof because it is unknown whether quantum computers need all these amplitudes. That is, if quantum computers can function with much fewer amplitudes (a polynomial number instead of an exponential number in $n$), a classical computer would be able to keep track of all of them. In terms of complexity classes, the exponential number of amplitudes in a general entangled state is evidence that P $\neq$ BQP.

We can also use powers to simplify the notation. If we have $n$ qubits, each in the state $|0\rangle$, we can write the state as

$$|0\rangle^{\otimes n} = \underbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}_{n} = \underbrace{|0\rangle|0\rangle\ldots|0\rangle}_{n} = |\underbrace{00\ldots0}_{n}\rangle = |0^n\rangle.$$

With a single qubit, we could parameterize a state as

$$\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle,$$

with the coordinates $(\theta, \phi)$ interpreted as a point on the Bloch sphere. With two qubits, however, we have four complex amplitudes $c_0$, $c_1$, $c_2$, $c_3$ (although one can

be made real by factoring out an global phase), and unfortunately, this is too many parameters to represent in three-dimensions. There is no Bloch sphere representation for a general multi-qubit state.

The tensor product also works for bras, so

$$\langle 0| \otimes \langle 0| = \langle 0|\langle 0| = \langle 00|.$$

Then, the inner product of, say $\langle 01|$ and $|00\rangle$, is obtained by matching up qubits. For example,

$$\langle 01|00\rangle = \underbrace{\langle 0|0\rangle}_{1} \cdot \underbrace{\langle 1|0\rangle}_{0} = 0.$$

So $|01\rangle$ and $|00\rangle$ are orthogonal.

---

**Exercise 4.3.** Calculate the following inner products:
(a) $\langle 10|11\rangle$.
(b) $\langle +-|01\rangle$.
(c) $\langle 1+0|1-0\rangle$.

---

### *4.2.2 Kronecker Product*

In linear algebra, the tensor product is simply the *Kronecker product*, which is obtained by multiplying each term of the first matrix/vector by the entire second matrix/vector. For example, with two qubits,

$$|00\rangle = |0\rangle|0\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0\begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

$$|01\rangle = |0\rangle|1\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0\begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

$$|10\rangle = |1\rangle|0\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1\begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

$$|11\rangle = |1\rangle|1\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0\begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 1\begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Then,

$$c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix}.$$

Similarly, with three qubits, its state can be written as a column vector with eight elements:

$$\sum_{j=0}^{7} c_j|j\rangle = c_0|0\rangle + c_1|1\rangle + \cdots + c_7|7\rangle = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_7 \end{pmatrix}.$$

With $n$ qubits, the vector has $N = 2^n$ elements:

$$|\psi\rangle = \sum_{j=0}^{N-1} c_j|j\rangle = c_0|0\rangle + c_1|1\rangle + \cdots + c_{N-1}|N-1\rangle = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{N-1} \end{pmatrix}.$$

With bras, the Kronecker product is still the tensor product. For example,

$$\langle 00| = \langle 0| \otimes \langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 1 & 0 \end{pmatrix} & 0\begin{pmatrix} 1 & 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}.$$

So, a general quantum state of $n$ qubits, written as a bra, is

$$\langle \psi| = \sum_{j=0}^{N-1} c_j^* \langle j| = c_0^*\langle 0| + c_1^*\langle 1| + \cdots + c_{N-1}^*\langle N-1| = \begin{pmatrix} c_0^* & c_1^* & \cdots & c_{N-1}^* \end{pmatrix}.$$

---

**Exercise 4.4.** Verify that

$$|1\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

---

**Exercise 4.5.** Consider a two-qubit state

$$|\psi\rangle = \frac{1}{2}|00\rangle + \frac{i}{\sqrt{2}}|10\rangle + \frac{\sqrt{3}+i}{4}|11\rangle.$$

(a) What is $|\psi\rangle$ as a (column) vector?
(a) What is $\langle\psi|$ as a (row) vector?

---

**Exercise 4.6.** Show that $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ is a complete orthonormal basis for the state of two qubits by showing that it satisfies the completeness relation

$$|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11| = I,$$

where $I$ is the $4 \times 4$ identity matrix:

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

### 4.2.3 Measuring Individual Qubits

Say we have two qubits in the state

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|01\rangle + \frac{\sqrt{3}}{4}|10\rangle + \frac{1}{4}|11\rangle.$$

If we measure both qubits, we would get $|00\rangle$ with probability $1/2$, $|01\rangle$ with probability $1/4$, $|10\rangle$ with probability $3/16$, or $|11\rangle$ with probability $1/16$.

Now, instead of measuring both qubits, let us only measure the left qubit. This yields $|0\rangle$ or $|1\rangle$ with some probabilities, and the state collapses to some state, so the outcomes are

$|0\rangle$ with some probability, and the state collapses to something,

$|1\rangle$ with some probability, and the state collapses to something.

The probability of getting $|0\rangle$ when measuring the left qubit is given by the sum of the norm-squares of the amplitudes of $|00\rangle$ and $|01\rangle$, since those both have the left qubit as $|0\rangle$. That is, the probability of getting $|0\rangle$ is

$$\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{2}\right|^2 = \frac{3}{4}.$$

Similarly, if the outcome is $|1\rangle$, then from the $|10\rangle$ and $|11\rangle$ states, the probability is

$$\left|\frac{\sqrt{3}}{4}\right|^2 + \left|\frac{1}{4}\right|^2 = \frac{1}{4}.$$

Then, the results of the measurement are:

$|0\rangle$ with probability $\frac{3}{4}$, and the state collapses to something,

$|1\rangle$ with probability $\frac{1}{4}$, and the state collapses to something.

Now for the states after measurement, if the outcome is $|0\rangle$, then the state collapses to the parts where the left qubit is $|0\rangle$, so it becomes

$$A\left(\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{2}|01\rangle\right),$$

where $A$ is a normalization constant. Similarly, if the outcome is $|1\rangle$, then the state collapses to the terms where the left qubit is $|1\rangle$, so it becomes

$$B\left(\frac{\sqrt{3}}{4}|10\rangle+\frac{1}{4}|11\rangle\right).$$

where $B$ is a normalization constant. Normalizing these, we get $A=2/\sqrt{3}$ and $B=2$, so measuring the left qubit yields

$$|0\rangle \text{ with probability } \frac{3}{4}, \text{ and the state collapses to } \sqrt{\frac{2}{3}}|00\rangle+\frac{1}{\sqrt{3}}|01\rangle,$$
$$|1\rangle \text{ with probability } \frac{1}{4}, \text{ and the state collapses to } \frac{\sqrt{3}}{2}|10\rangle+\frac{1}{2}|11\rangle.$$

We can apply these ideas to any number of qubits. For example, if we have three qubits in the state

$$c_0|000\rangle+c_1|001\rangle+c_2|010\rangle+c_3|011\rangle+c_4|100\rangle+c_5|101\rangle+c_6|110\rangle+c_7|111\rangle,$$

and we measure the left and middle qubits, the possible outcomes are

$$|00\rangle \text{ with probability } |c_0|^2+|c_1|^2, \text{ collapses to } \frac{c_0|000\rangle+c_1|001\rangle}{\sqrt{|c_0|^2+|c_1|^2}},$$
$$|01\rangle \text{ with probability } |c_2|^2+|c_3|^2, \text{ collapses to } \frac{c_2|010\rangle+c_3|011\rangle}{\sqrt{|c_2|^2+|c_3|^2}},$$
$$|10\rangle \text{ with probability } |c_4|^2+|c_5|^2, \text{ collapses to } \frac{c_4|100\rangle+c_5|101\rangle}{\sqrt{|c_4|^2+|c_5|^2}},$$
$$|11\rangle \text{ with probability } |c_6|^2+|c_7|^2, \text{ collapses to } \frac{c_6|110\rangle+c_7|111\rangle}{\sqrt{|c_6|^2+|c_7|^2}}.$$

---

**Exercise 4.7.** Two qubits are in the state

$$\frac{i}{\sqrt{10}}|00\rangle+\frac{1-2i}{\sqrt{10}}|01\rangle+\frac{e^{i\pi/100}}{\sqrt{10}}|10\rangle+\frac{\sqrt{3}}{\sqrt{10}}|11\rangle.$$

If we measure the qubits in the $Z$-basis $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$, what are the possible outcomes and with what probabilities?

---

**Exercise 4.8.** Normalize the following quantum state:

$$A\left(\frac{1}{2}|00\rangle+i|01\rangle+\sqrt{2}|10\rangle-|11\rangle\right).$$

---

### 4.2.4 Sequential Single-Qubit Measurements

We have answered the question of what happens when we measure just a single qubit or a subset of qubits. Now, let us take this a step further and consider what happens if we measure the qubits, one after another. For example, in the last section, we started with two qubits in the state

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|01\rangle + \frac{\sqrt{3}}{4}|10\rangle + \frac{1}{4}|11\rangle.$$

If we first measure the left qubit, we get

$$|0\rangle \text{ with probability } \frac{3}{4}, \text{ and the state collapses to } \sqrt{\frac{2}{3}}|00\rangle + \frac{1}{\sqrt{3}}|01\rangle,$$
$$|1\rangle \text{ with probability } \frac{1}{4}, \text{ and the state collapses to } \frac{\sqrt{3}}{2}|10\rangle + \frac{1}{2}|11\rangle.$$

Now if we measure the right qubit after this, the possible outcomes for the sequence of measurements are $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. The probability of getting $|00\rangle$ is the probability of first getting $|0\rangle$ for the left qubit, which was $3/4$, times the probability of getting $|0\rangle$ for the right qubit, which is $2/3$ because the state collapsed after the first measurement. Multiplying these, the probability of getting $|00\rangle$ is $(3/4)(2/3) = 2/4 = 1/2$. We can perform this calculation for every possible outcome:

$$\text{Prob}(|00\rangle) = \text{Prob}(\text{first left } |0\rangle)\,\text{Prob}(\text{then right } |0\rangle) = \frac{3}{4}\frac{2}{3} = \frac{1}{2},$$
$$\text{Prob}(|01\rangle) = \text{Prob}(\text{first left } |0\rangle)\,\text{Prob}(\text{then right } |1\rangle) = \frac{3}{4}\frac{1}{3} = \frac{1}{4},$$
$$\text{Prob}(|10\rangle) = \text{Prob}(\text{first left } |1\rangle)\,\text{Prob}(\text{then right } |0\rangle) = \frac{1}{4}\frac{3}{4} = \frac{3}{16},$$
$$\text{Prob}(|11\rangle) = \text{Prob}(\text{first left } |1\rangle)\,\text{Prob}(\text{then right } |1\rangle) = \frac{1}{4}\frac{1}{4} = \frac{1}{16}.$$

Notice these outcomes and probabilities are exactly the same as if we had measured both qubits at the same time, as they should be. Measuring both qubits is the same as measuring one after another, assuming the state was not modified between the two measurements.

---

**Exercise 4.9.** Consider the two-qubit state

$$\frac{1}{4}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle.$$

If you measure only the left qubit, what are the resulting states, and with what probabilities?

---

**Exercise 4.10.** Consider the three-qubit state

$$\frac{1}{6}|000\rangle + \frac{1}{3\sqrt{2}}|001\rangle + \frac{1}{\sqrt{6}}|010\rangle + \frac{1}{2}|011\rangle + \frac{1}{6}|100\rangle + \frac{1}{3}|101\rangle + \frac{1}{6}|110\rangle + \frac{1}{\sqrt{3}}|111\rangle.$$

If you measure only the left and right qubits, but not the middle qubit, what are the resulting states, and with what probabilities?

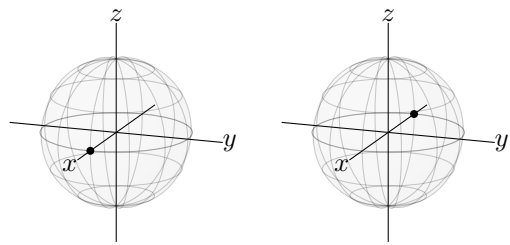
## 4.3 Entanglement

### *4.3.1 Product States*

Some quantum states can be factored into (the tensor product of) individual qubit states. For example,

$$\begin{aligned}\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) &= \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}_{|+\rangle} \otimes \underbrace{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)}_{|-\rangle} \\ &= |+\rangle \otimes |-\rangle \\ &= |+\rangle|-\rangle.\end{aligned}$$

To confirm this to yourself, work it out in reverse order by multiplying out the states and showing that you get the original state. Such factorizable states are called *product states* or *simply separable states*. Each single-qubit state can be visualized on the Bloch sphere, so $|+\rangle|-\rangle$ would be two Bloch spheres, with the first at the $x$-axis, and the other at the $-x$-axis:




Let us work through an example of how to factor a state. Say two qubits are in the state

$$\frac{1}{2\sqrt{2}}\left(\sqrt{3}|00\rangle - \sqrt{3}|01\rangle + |10\rangle - |11\rangle\right).$$

We want to write this as the product of two single-qubit states,

$$|\psi_1\rangle|\psi_0\rangle,$$

where

$$|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle, \quad |\psi_0\rangle = \alpha_0|0\rangle + \beta_0|1\rangle.$$

Then,

$$\begin{aligned}|\psi_1\rangle|\psi_0\rangle &= (\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_0|0\rangle + \beta_0|1\rangle) \\ &= \alpha_1\alpha_0|00\rangle + \alpha_1\beta_0|01\rangle + \beta_1\alpha_0|10\rangle + \beta_1\beta_0|11\rangle.\end{aligned}$$

Matching up the coefficients with our original state,

$$\alpha_1\alpha_0 = \frac{\sqrt{3}}{2\sqrt{2}}, \quad \alpha_1\beta_0 = \frac{-\sqrt{3}}{2\sqrt{2}}, \quad \beta_1\alpha_0 = \frac{1}{2\sqrt{2}}, \quad \beta_1\beta_0 = \frac{-1}{2\sqrt{2}}.$$

Using these equations, let us solve for the variables in terms of one of them. Starting with the first equation, we can solve for $\alpha_1$ in terms of $\alpha_0$:

$$\alpha_1 = \frac{\sqrt{3}}{2\sqrt{2}\alpha_0}.$$

Plugging this into the second equation, we can solve for $\beta_0$ in terms of $\alpha_0$:

$$\beta_0 = -\alpha_0.$$

For the third equation, we can solve for $\beta_1$ in terms of $\alpha_0$:

$$\beta_1 = \frac{1}{2\sqrt{2}\alpha_0}.$$

Finally, plugging in $\beta_1 = 1/2\sqrt{2}\alpha_0$ and $\beta_0 = -\alpha_0$ into the fourth equation, we get

$$\frac{-1}{2\sqrt{2}} = \frac{-1}{2\sqrt{2}},$$

which is a true statement, so it is satisfied, although it does not tell us anything new. So, we have solved for $\alpha_1$, $\beta_1$, and $\beta_0$ in terms of $\alpha_0$, and this is actually sufficient. Plugging into the product state,

$$\begin{aligned}|\psi_1\rangle|\psi_0\rangle &= (\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_0|0\rangle + \beta_0|1\rangle) \\ &= \left(\frac{\sqrt{3}}{2\sqrt{2}\alpha_0}|0\rangle + \frac{1}{2\sqrt{2}}\frac{1}{\alpha_0}|1\rangle\right)(\alpha_0|0\rangle - \alpha_0|1\rangle).\end{aligned}$$

We see that $\alpha_0$ cancels, yielding

$$|\psi_1\rangle|\psi_0\rangle = \left(\frac{\sqrt{3}}{2\sqrt{2}}|0\rangle + \frac{1}{2\sqrt{2}}|1\rangle\right)(|0\rangle - |1\rangle).$$

Moving the factor of $1/\sqrt{2}$ to the right qubit so that both qubits are normalized,

$$|\psi_1\rangle|\psi_0\rangle = \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right).$$

Thus, the left qubit is in the state $\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$, and the right qubit is in the state $|-\rangle$.

In general, a product state of $n$ qubits can be written

$$(\alpha_{n-1}|0\rangle + \beta_{n-1}|1\rangle) \otimes \cdots \otimes (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_0|0\rangle + \beta_0|1\rangle).$$

This only has $2n$ amplitudes, so a classical computer can efficiently store the amplitudes of product states. If quantum computers only used product states, they would be efficiently simulated by classical computers.

### 4.3.2 Entangled States

There exist quantum states that cannot be factored into product states. These are called *entangled states*. For example, with two qubits,

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

cannot be written as $|\psi_1\rangle|\psi_0\rangle$. As a proof, let us try writing it as a product state using the procedure from the last section:

$$\begin{aligned}|\psi_1\rangle|\psi_0\rangle &= (\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_0|0\rangle + \beta_0|1\rangle) \\ &= \alpha_1\alpha_0|00\rangle + \alpha_1\beta_0|01\rangle + \beta_1\alpha_0|10\rangle + \beta_1\beta_0|11\rangle.\end{aligned}$$

Matching the coefficients, we get

$$\alpha_1\alpha_0 = \frac{1}{\sqrt{2}}, \quad \alpha_1\beta_0 = 0, \quad \beta_1\alpha_0 = 0, \quad \beta_1\beta_0 = \frac{1}{\sqrt{2}}.$$

The second equation requires $\alpha_1 = 0$ or $\beta_0 = 0$. If $\alpha_1 = 0$, then the first equation gives $0 = 1/\sqrt{2}$, which is false. If $\beta_0 = 0$, then the fourth equation gives $0 = 1/\sqrt{2}$. Thus, there is no solution to these four equations, so $|\Phi^+\rangle$ cannot be written as a product state. It is an entangled state. This property that the state of the qubits are intertwined is called *entanglement*.

Since an entangled state cannot be factored, a general entangled state of $n$ qubits would have $N = 2^n$ amplitudes $c_0$ through $c_{N-1}$:

$$|\psi\rangle = \sum_{j=0}^{N-1} c_j|j\rangle = c_0|0\rangle + c_1|1\rangle + \cdots + c_{N-1}|N-1\rangle = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{N-1} \end{pmatrix}.$$

In the Entanglion board game, the planets within the Entanglion galaxy correspond to two-qubit states that are entangled. Planet Phi Plus is precisely $|\Phi^+\rangle$.

We will discuss entanglement in more detail in Chapter 6.

**Exercise 4.11.** Are each of the following states a product state or entangled state? If it is a product state, give the factorization.

(a) $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

(b) $\frac{1}{\sqrt{2}}(|10\rangle + i|11\rangle)$.

---

**Exercise 4.12.** Are each of the following states a product state or entangled state? If it is a product state, give the factorization.

(a) $\frac{1}{4}\left(3|00\rangle - \sqrt{3}|01\rangle + \sqrt{3}|10\rangle - |11\rangle\right)$.

(b) $\frac{1}{\sqrt{3}}|0\rangle|+\rangle + \sqrt{\frac{2}{3}}|1\rangle|-\rangle$.

---

## 4.4 Quantum Gates

### *4.4.1 One-Qubit Quantum Gates*

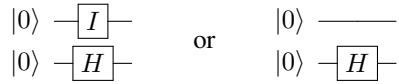
Say we have multiple qubits, and we want to apply a single-qubit gate (like $I$, $X$, $Y$, $Z$, $S$, $T$, or $H$) to just a single qubit. For example, say we have two qubits in the $|00\rangle = |0\rangle \otimes |0\rangle$ state, and we want to apply the Hadamard gate to the left qubit, but leave the right qubit alone (i.e., apply the identity gate to it). We write the gates using a tensor product, so we write

$$\begin{aligned}(H \otimes I)(|0\rangle \otimes |0\rangle) &= H|0\rangle \otimes I|0\rangle \\ &= |+\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle).\end{aligned}$$

Compressing the notation and also writing the result as a column vector,

$$(H \otimes I)|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\1\\0\end{pmatrix}.$$

To draw as a quantum circuit, we use the convention that the rightmost qubit corresponds to the top row of the quantum circuit, and the leftmost qubit corresponds to the bottom row of the quantum circuit:



We follow this convention so that it matches Quirk, and in Chapter 5 the IBM Quantum Composer. Nielsen and Chuang follows the opposite convention, where the leftmost qubit corresponds to the top row of the quantum circuit.

We can find $H \otimes I$ as a matrix a couple different ways. First, we can find how $H \otimes I$ acts on each of the basis states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. We already found how it acts on $|00\rangle$ above. Continuing with the rest,

$$(H \otimes I)|01\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix},$$

$$(H \otimes I)|10\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix},$$

$$(H \otimes I)|11\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \end{pmatrix}.$$

As in Section 3.3.1, we can write $H \otimes I$ as a matrix by combining the column vectors for $(H \otimes I)|00\rangle, \ldots, (H \otimes I)|11\rangle$ as a $4 \times 4$ grid:

$$H \otimes I = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

The second way to find this matrix is by taking the Kronecker product of $H$ and $I$:

$$H \otimes I = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & 1 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & -1 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

This matches what we previously obtained. We can also find the Kronecker product using Mathematica or SageMath:

- In Mathematica,

```
H=1/Sqrt[2]*{{1,1},{1,-1}};
eye={{1,0},{0,1}};
KroneckerProduct[H,eye]
```

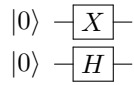
- In SageMath,

```
sage: H = 1/sqrt(2) * Matrix([[1,1],[1,-1]])
sage: eye = Matrix([[1,0],[0,1]])
sage: H.tensor_product(eye)
```

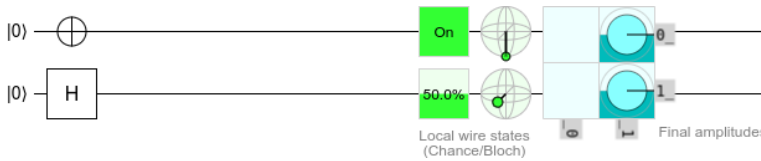
As another example, to act on the left qubit with $H$ and the right qubit with $X$, we would write $H \otimes X$, so

$$(H \otimes X)|0\rangle|0\rangle = |+\rangle|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle).$$

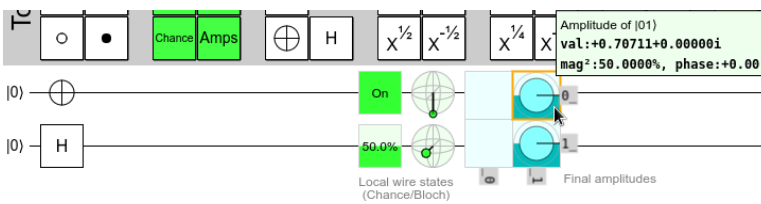
As a quantum circuit, we would draw this as




Simulating this in Quirk, we get




This is consistent with the state $|+\rangle|1\rangle$. Since the right/top qubit is $|1\rangle$, Quirk correctly shows that the probability of getting $|1\rangle$ when measuring it is 100% (On), and it correctly draws the state at the south pole of the Bloch sphere. Similarly, the left/bottom qubit is $|+\rangle$, and Quirk correctly shows that the probability of measuring it to be $|1\rangle$ is 50%, and it correctly draws the state at the $x$-axis of the Bloch sphere. In additional, Quirk also depicts the amplitudes on the real-imaginary plane, labeled "Final amplitudes." There are four boxes, and the top-left box depicts the amplitude of $|00\rangle$, which is zero, and the top-right box depicts the amplitude of $|01\rangle$, which is $1/\sqrt{2}$. Since this is real, it corresponds to a vector pointing along the real axis of the real-imaginary plane. The background is also half filled, indicating a probability of $|1/\sqrt{2}|^2 = 1/2$. Mousing over, we get




and the amplitude is also explicitly given as $0.70711 = 1/\sqrt{2}$, which has a phase or angle of $0^\circ$ on the real-imaginary plane since it is purely real, and a norm-square magnitude of 50%. The bottom-left box depicts the amplitude of $|10\rangle$, which is zero, and finally the bottom-right box depicts the amplitude of $|11\rangle$, which is $1/\sqrt{2}$.

As a third example, if we have $n$ qubits, and we want to apply $H$ to all $n$ qubits, we can write $H \otimes H \otimes \cdots \otimes H$ as $H^{\otimes n}$. For example,

$$H^{\otimes n}|0\rangle^{\otimes n} = |+\rangle^{\otimes n}.$$

Note one-qubit gates are unable to create entangled states because each qubit evolves independently of the others. To create entanglement, we need quantum gates that operate on multiple qubits at a time.

---

**Exercise 4.13.** In this problem, you will prove some of the game mechanics of Entanglion. Please refer to Fig. 4.1 for the game board. If the players are on planet Psi Plus, and either player uses an X engine card, they both move to planet Phi Plus, and vice versa. Similarly, if the players are on planet Psi Minus, and either player uses an X engine card, they both move to planet Phi Minus, and vice versa. These planets correspond to the following states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

(a) Show that when the $X$ gate is applied to either qubit of $|\Psi^+\rangle$, the result is $|\Phi^+\rangle$, up to a global phase.
(b) Show that when the $X$ gate is applied to either qubit of $|\Phi^+\rangle$, the result is $|\Psi^+\rangle$, up to a global phase.
(c) Show that when the $X$ gate is applied to either qubit of $|\Psi^-\rangle$, the result is $|\Phi^-\rangle$, up to a global phase.
(d) Show that when the $X$ gate is applied to either qubit of $|\Phi^-\rangle$, the result is $|\Psi^-\rangle$, up to a global phase.

---

**Exercise 4.14.** Answer the following questions.
(a) What is $H \otimes X$ as a $4 \times 4$ matrix?
(b) Consider

$$|\psi\rangle = \frac{1}{4}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle.$$

What is $(H \otimes X)|\psi\rangle$? Hint: You may use a computer.

---

### *4.4.2 Two-Qubit Quantum Gates*

Quantum gates can also operate on two qubits at the same time. Some important examples include:

- The *CNOT gate* or *controlled-NOT gate* inverts the right qubit if the left qubit is 1:

$$\begin{aligned}
\text{CNOT}|00\rangle &= |00\rangle,\\
\text{CNOT}|01\rangle &= |01\rangle,\\
\text{CNOT}|10\rangle &= |11\rangle,\\
\text{CNOT}|11\rangle &= |10\rangle.
\end{aligned}$$

The left qubit is called the *control qubit*, and the right qubit is called the *target qubit*. Note the control qubit is unchanged by CNOT, whereas the target qubit becomes the XOR (exclusive OR) of the inputs:

$$\text{CNOT}|a\rangle|b\rangle = |a\rangle|a \oplus b\rangle.$$

Thus, CNOT is a quantum XOR gate. Also, since the $X$ gate is the NOT gate, the CNOT gate is also called the C$X$ gate or *controlled-X gate*.
In Entanglion (see Fig. 4.1), the player who uses the CNOT engine card is the target qubit, and the other player is the control qubit. So, you can move between planets Zero and One by playing a CNOT engine card when the other player is at One.
Acting on a superposition,

$$\begin{aligned}
&\text{CNOT}\,(c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle)\\
&\quad = c_0\text{CNOT}|00\rangle + c_1\text{CNOT}|01\rangle + c_2\text{CNOT}|10\rangle + c_3\text{CNOT}|11\rangle\\
&\quad = c_0|00\rangle + c_1|01\rangle + c_2|11\rangle + c_3|10\rangle\\
&\quad = c_0|00\rangle + c_1|01\rangle + c_3|10\rangle + c_2|11\rangle.
\end{aligned}$$

So, the amplitudes of $|10\rangle$ and $|11\rangle$ are swapped.
As a matrix, the columns correspond to CNOT acting on $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$:

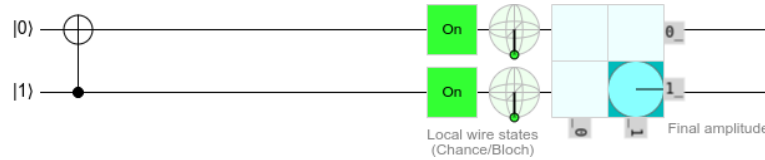
$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

For example, acting on a general superposition,

$$\text{CNOT}\,(c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle) = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} c_0\\ c_1\\ c_2\\ c_3 \end{pmatrix} = \begin{pmatrix} c_0\\ c_1\\ c_3\\ c_2 \end{pmatrix}.$$

So, the amplitudes of $|10\rangle$ and $|11\rangle$ are swapped, as expected.
As a quantum circuit, CNOT spans two qubits or two lines:

The solid dot indicates control, and the $\oplus$ denotes the target, which is the XOR of the control and the target. Simulating this in Quirk, we drag an $X$ gate onto the top line and a "Control" solid dot, which is in the top Toolbox under "Probes," onto the bottom line:




We also clicked on the initial state of the control qubit to change it to $|1\rangle$ (alternatively, we could leave the initial state as $|0\rangle$ and apply $X$ to it, resulting in $|1\rangle$). This triggers the CNOT, changing the target from $|0\rangle$ to $|1\rangle$. The result is that both qubits are "On" with 100% probability. They are both at the south poles of their Bloch spheres, and the amplitude of $|11\rangle$ is 1.
To further clarify the control and target qubits, we may write CNOT with subscripts:

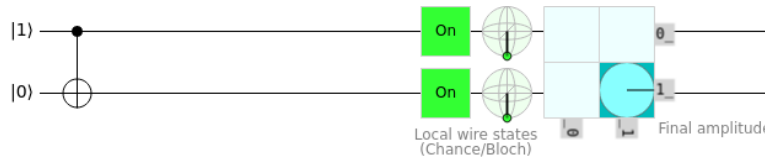
$$\text{CNOT}_{ij} = \text{CNOT with qubit } i \text{ as the control and qubit } j \text{ as the target.}$$

Since we label the qubits from right-to-left starting with 0, we have been using

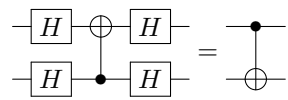
$$\text{CNOT} = \text{CNOT}_{10}.$$

If we instead want the control and target to be flipped, it would be $\text{CNOT}_{01}$, and we would draw the circuit as

To simulate this in Quirk, we just put the control on the zeroth qubit and the $X$ gate on the first qubit:




We set the control qubit to $|1\rangle$, and so the CNOT gate flipped the target to $|1\rangle$. Another way to flip the control and target qubits is to apply Hadamard gates to both sides of the CNOT:




In other words,

$$(H \otimes H)\text{CNOT}(H \otimes H) = \text{CNOT}_{01}$$

We can prove this circuit identity using either elementary algebra or linear algebra. First, using elementary algebra, the right-hand-side of equation yields the following when applied to a superposition of the $Z$-basis states:

$$\begin{aligned}
&\mathrm{CNOT}_{01}\left(c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle\right) \\
&\qquad = c_0|00\rangle + c_1|11\rangle + c_2|10\rangle + c_3|01\rangle \\
&\qquad = \left(c_0|00\rangle + c_3|01\rangle + c_2|10\rangle + c_1|11\rangle\right).
\end{aligned}$$

Let us show that the left-hand-side yields the same state:

$$\begin{aligned}
&c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle \\
&\quad \xrightarrow{H\otimes H} c_0|{+}{+}\rangle + c_1|{+}{-}\rangle + c_2|{-}{+}\rangle + c_3|{-}{-}\rangle \\
&\quad = \frac{c_0}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) + \frac{c_1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right) \\
&\qquad + \frac{c_2}{2}\left(|00\rangle + |01\rangle - |10\rangle - |11\rangle\right) + \frac{c_3}{2}\left(|00\rangle - |01\rangle - |10\rangle + |11\rangle\right) \\
&\quad = \frac{1}{2}\left(c_0 + c_1 + c_2 + c_3\right)|00\rangle + \frac{1}{2}\left(c_0 - c_1 + c_2 - c_3\right)|01\rangle \\
&\qquad + \frac{1}{2}\left(c_0 + c_1 - c_2 - c_3\right)|10\rangle + \frac{1}{2}\left(c_0 - c_1 - c_2 + c_3\right)|11\rangle \\
&\quad \xrightarrow{\mathrm{CNOT}} \frac{1}{2}\left(c_0 + c_1 + c_2 + c_3\right)|00\rangle + \frac{1}{2}\left(c_0 - c_1 + c_2 - c_3\right)|01\rangle \\
&\qquad + \frac{1}{2}\left(c_0 + c_1 - c_2 - c_3\right)|11\rangle + \frac{1}{2}\left(c_0 - c_1 - c_2 + c_3\right)|10\rangle \\
&\quad = \frac{1}{2}\left(c_0 + c_1 + c_2 + c_3\right)|00\rangle + \frac{1}{2}\left(c_0 - c_1 + c_2 - c_3\right)|01\rangle \\
&\qquad + \frac{1}{2}\left(c_0 - c_1 - c_2 + c_3\right)|10\rangle + \frac{1}{2}\left(c_0 + c_1 - c_2 - c_3\right)|11\rangle \\
&\quad \xrightarrow{H\otimes H} \frac{1}{4}\left(c_0 + c_1 + c_2 + c_3\right)|{+}{+}\rangle + \frac{1}{4}\left(c_0 - c_1 + c_2 - c_3\right)|{+}{-}\rangle \\
&\qquad + \frac{1}{4}\left(c_0 - c_1 - c_2 + c_3\right)|{-}{+}\rangle + \frac{1}{4}\left(c_0 + c_1 - c_2 - c_3\right)|{-}{-}\rangle \\
&\quad = \frac{1}{4}\left(c_0 + c_1 + c_2 + c_3\right)\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \\
&\qquad + \frac{1}{4}\left(c_0 - c_1 + c_2 - c_3\right)\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right) \\
&\qquad + \frac{1}{4}\left(c_0 - c_1 - c_2 + c_3\right)\left(|00\rangle + |01\rangle - |10\rangle - |11\rangle\right) \\
&\qquad + \frac{1}{4}\left(c_0 + c_1 - c_2 - c_3\right)\left(|00\rangle - |01\rangle - |10\rangle + |11\rangle\right) \\
&\quad = c_0|00\rangle + c_3|01\rangle + c_2|10\rangle + c_1|11\rangle.
\end{aligned}$$

This is the same state, and so we have proved the circuit identity. It was rather tedious, however. Proving the circuit identity using linear algebra is easier. First,

note that

$$\text{CNOT}_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

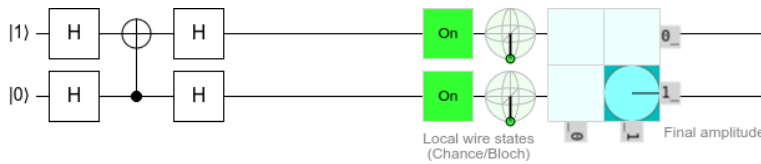
since its columns show that $|00\rangle$ stays $|00\rangle$, $|01\rangle$ becomes $|11\rangle$, $|10\rangle$ stays $|10\rangle$, and $|11\rangle$ becomes $|01\rangle$. Now, let us show that $(H \otimes H)\text{CNOT}(H \otimes H)$ corresponds to the same matrix. First,

$$H \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Then,

$$\begin{aligned} &(H \otimes H)\text{CNOT}(H \otimes H) \\ &\quad = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \\ &\quad = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \\ &\quad = \frac{1}{4} \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 4 & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix} \\ &\quad = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \end{aligned}$$

This is precisely $\text{CNOT}_{01}$, and so we have proved the circuit identity using linear algebra. We also could have computed it using Mathematica or SageMath. Simulating the identity in Quirk,



Since the top qubit is initially $|1\rangle$, and it is now the control qubit, the bottom qubit gets flipped to $|1\rangle$. So, both qubits are "On."

The CNOT gate is important because it can produce entanglement. For example,

$$\begin{aligned}
\text{CNOT}|+\rangle|0\rangle &= \text{CNOT}\frac{1}{\sqrt{2}}(|00\rangle+|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) = |\Phi^+\rangle,\\
\text{CNOT}|-\rangle|0\rangle &= \text{CNOT}\frac{1}{\sqrt{2}}(|00\rangle-|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle) = |\Phi^-\rangle,\\
\text{CNOT}|+\rangle|1\rangle &= \text{CNOT}\frac{1}{\sqrt{2}}(|01\rangle+|11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle) = |\Psi^+\rangle,\\
\text{CNOT}|-\rangle|1\rangle &= \text{CNOT}\frac{1}{\sqrt{2}}(|01\rangle-|11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) = |\Psi^-\rangle.
\end{aligned}$$

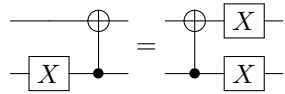
In Section 4.3.2, we proved that $|\Phi^+\rangle$ is entangled. It can be shown that the other three states, $|\Phi^-\rangle$, $|\Psi^+\rangle$, and $|\Psi^-\rangle$, are also entangled. So, in each of the above four calculations, we started with product states and ended up with entangled states. This demonstrates that CNOT can create entanglement. The four states, $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, and $|\Psi^-\rangle$, are known as the *Bell states* or *EPR states* or *EPR pairs* (for Einstein, Podolsky, and Rosen). They form an orthonormal basis called the *Bell basis* (see Exercise 4.19), and they will be important in Chapter 6.

In Entanglion (see Fig. 4.1), the player who uses the CNOT engine card is the target qubit, and the other player is the control qubit. So, playing a CNOT engine card while at planet Zero, while your teammate is at planet Plus, causes both of you to move to planet Phi Plus. Similarly, the spaceships go from planets Zero and Minus to Phi Minus, One and Plus to Psi Plus, and One and Minus to Psi Minus.

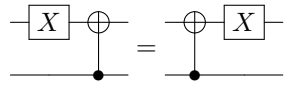
---

**Exercise 4.15.** Prove the following circuit identities, such as by finding the matrix representation of each circuit.

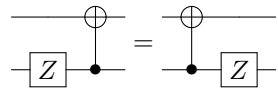
(a) $\text{CNOT}(X\otimes I) = (X\otimes X)\text{CNOT}$.



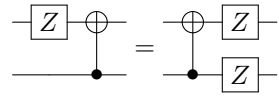

(b) $\text{CNOT}(I\otimes X) = (I\otimes X)\text{CNOT}$.



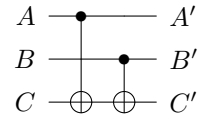

(c) $\text{CNOT}(Z\otimes I) = (Z\otimes I)\text{CNOT}$.




(d) $\text{CNOT}(I\otimes Z) = (Z\otimes Z)\text{CNOT}$.

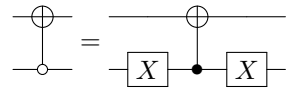



**Exercise 4.16.** Consider the following circuit, which consists of two CNOTs.




(a) What is the truth table for this circuit?
(b) How does it compare to the reversible circuit for XOR in Exercise 1.43?

**Exercise 4.17.** Recall CNOT flips the right qubit if the left qubit is 1. The *anti-controlled-NOT gate* flips the right qubit if the left qubit is 0. As a quantum circuit, the anti-control is drawn as an open dot instead of a solid dot. Prove that it can be obtained from an ordinary CNOT by applying an $X$ gate to each side of the control:




**Exercise 4.18.** If we apply CNOT in the $Z$-basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, the left qubit acts as the control and the right qubit acts as the target. In this problem, we will prove that in the $X$-basis $\{|{+}{+}\rangle, |{+}{-}\rangle, |{-}{+}\rangle, |{-}{-}\rangle$, if the right qubit is $|-\rangle$, the left qubit gets flipped between $|+\rangle$ and $|-\rangle$, so the control and target are reversed. That is,

$$\begin{aligned}
\text{CNOT}|+\rangle|+\rangle &= |+\rangle|+\rangle,\\
\text{CNOT}|+\rangle|-\rangle &= |-\rangle|-\rangle,\\
\text{CNOT}|-\rangle|+\rangle &= |-\rangle|+\rangle,\\
\text{CNOT}|-\rangle|-\rangle &= |+\rangle|-\rangle.
\end{aligned}$$

To prove these four equations, we start with the circuit identity from the main text:

$$(H\otimes H)\text{CNOT}(H\otimes H) = \text{CNOT}_{01}.$$

Then, we multiply on the left and on the right by $H\otimes H$:

$$(H\otimes H)(H\otimes H)\text{CNOT}(H\otimes H)(H\otimes H) = (H\otimes H)\text{CNOT}_{01}(H\otimes H).$$

Since $H^2 = I$, this becomes

$$(I\otimes I)\text{CNOT}(I\otimes I) = (H\otimes H)\text{CNOT}_{01}(H\otimes H).$$

Dropping the identity matrices,

$$\text{CNOT} = (H\otimes H)\text{CNOT}_{01}(H\otimes H).$$

Now it is straightforward to prove how CNOT acts in the $X$-basis. Beginning with $|{+}{+}\rangle$,

$$\begin{aligned}
\text{CNOT}|+\rangle|+\rangle &= (H\otimes H)\text{CNOT}_{01}(H\otimes H)|+\rangle|+\rangle\\
&= (H\otimes H)\text{CNOT}_{01}|0\rangle|0\rangle\\
&= (H\otimes H)|0\rangle|0\rangle\\
&= |+\rangle|+\rangle.
\end{aligned}$$

Work out how CNOT acts on the remaining three basis states $|{+}{-}\rangle$, $|{-}{+}\rangle$, and $|{-}{-}\rangle$.

**Exercise 4.19.** Prove that the Bell basis satisfies the completeness relation:

$$|\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-| = I,$$

where $I$ is the $4 \times 4$ identity matrix.

---

- Just like CNOT, the *controlled-U* gate applies some quantum gate $U$ to the right qubit if the left qubit is 1:

$$\begin{aligned}
\mathrm{C}U|00\rangle &= |00\rangle,\\
\mathrm{C}U|01\rangle &= |01\rangle,\\
\mathrm{C}U|10\rangle &= |1\rangle \otimes U|0\rangle,\\
\mathrm{C}U|11\rangle &= |1\rangle \otimes U|1\rangle.
\end{aligned}$$

To get the matrix representation of C$U$, first say $U$ acts on a single qubit as

$$\begin{aligned}
U|0\rangle &= a|0\rangle + b|1\rangle,\\
U|1\rangle &= c|0\rangle + d|1\rangle.
\end{aligned}$$

So, $U$ as a $2 \times 2$ matrix is

$$U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Then,

$$\begin{aligned}
\mathrm{C}U|00\rangle &= |00\rangle,\\
\mathrm{C}U|01\rangle &= |01\rangle,\\
\mathrm{C}U|10\rangle &= |1\rangle \otimes (a|0\rangle + b|1\rangle) = a|10\rangle + b|11\rangle,\\
\mathrm{C}U|11\rangle &= |1\rangle \otimes (c|0\rangle + d|1\rangle) = c|10\rangle + d|11\rangle.
\end{aligned}$$

Representing each of these as column vectors and putting them together, C$U$ as a $4 \times 4$ matrix is

$$\mathrm{C}U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & c \\ 0 & 0 & b & d \end{pmatrix}.$$

This agrees with

$$\mathrm{CNOT} = \mathrm{C}X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Some examples are controlled-$Z$ and controlled-phase:


---

**Exercise 4.20.** What is the controlled-$Z$ gate as a matrix?

---

- The *SWAP gate* simply swaps the two qubits:

$$\begin{aligned}\text{SWAP}|00\rangle &= |00\rangle,\\ \text{SWAP}|01\rangle &= |10\rangle,\\ \text{SWAP}|10\rangle &= |01\rangle,\\ \text{SWAP}|11\rangle &= |11\rangle.\end{aligned}$$

  In other words,

$$\text{SWAP}|a\rangle|b\rangle = |b\rangle|a\rangle.$$

  This gate cannot produce entanglement because, if the qubits are in a product state, swapping the factors results in a product state. Acting on a superposition,

$$\begin{aligned}&\text{SWAP}\left(c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle\right)\\ &\quad= c_0\text{SWAP}|00\rangle + c_1\text{SWAP}|01\rangle + c_2\text{SWAP}|10\rangle + c_3\text{SWAP}|11\rangle\\ &\quad= c_0|00\rangle + c_1|10\rangle + c_2|01\rangle + c_3|11\rangle\\ &\quad= c_0|00\rangle + c_2|01\rangle + c_1|10\rangle + c_3|11\rangle.\end{aligned}$$

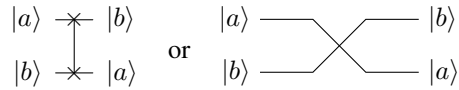
  So, the amplitudes of $|01\rangle$ and $|10\rangle$ are swapped.
  As a matrix, the columns correspond to SWAP acting on $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$:

$$\text{SWAP} = \begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}.$$

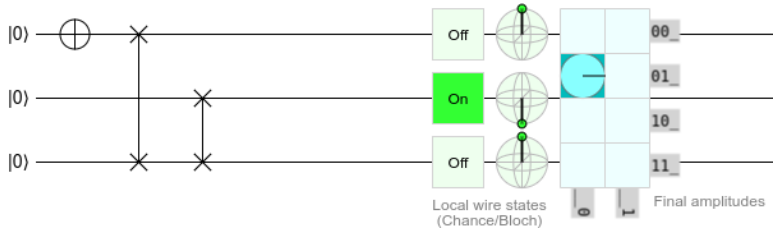
  For example, acting on a general superposition,

$$\text{SWAP}\left(c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle\right) = \begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}c_0\\c_1\\c_2\\c_3\end{pmatrix} = \begin{pmatrix}c_0\\c_2\\c_1\\c_3\end{pmatrix}.$$

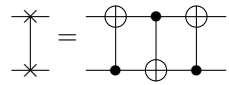
  So, the amplitudes of $|01\rangle$ and $|10\rangle$ are swapped, as expected.
  As a quantum circuit, we can draw a SWAP gate using a vertical line with $\times$'s at each end, or by literally swapping the wires:




  In Quirk, "Swap" is located in the top Toolbox under "Half Turns":




We also included an $X$ gate so that the top qubit is a $|1\rangle$. This swaps with the bottom qubit, which then swaps with the middle qubit, so the result is that the middle qubit is $|1\rangle$.
A SWAP gate can also be created using three CNOT gates:



Or as an equation,

$$\text{SWAP} = (\text{CNOT})(\text{CNOT}_{01})(\text{CNOT}).$$

As a proof, we can work through what each CNOT does and show that the result is a SWAP:

$$|a\rangle|b\rangle \xrightarrow{\text{CNOT}} |a\rangle|a\oplus b\rangle \xrightarrow{\text{CNOT}_{01}} |a\oplus a\oplus b\rangle|a\oplus b\rangle = |(a\oplus a)\oplus b\rangle|a\oplus b\rangle$$
$$= |0\oplus b\rangle|a\oplus b\rangle = |b\rangle|a\oplus b\rangle \xrightarrow{\text{CNOT}} |b\rangle|a\oplus b\oplus b\rangle = |b\rangle|a\rangle.$$

As another proof, we can multiply the three CNOTs as matrices and show that we get the matrix of a SWAP:

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} = \begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix} = \text{SWAP}.$$

---

**Exercise 4.21.** Entanglion contains four yellow planets besides the Bell States. Please see the game board at Fig. 4.1. They are labeled Omega Zero through Omega Three. These are not standard names, but they correspond to the quantum states

$$|\omega_0\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle),$$
$$|\omega_1\rangle = \frac{1}{2}(-|00\rangle + |01\rangle + |10\rangle + |11\rangle),$$
$$|\omega_2\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle),$$
$$|\omega_3\rangle = \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle).$$

The blue player corresponds to the left qubit, and the red player corresponds to the right qubit.
(a) Show that when the SWAP gate is applied to $|\omega_0\rangle$, we get $|\omega_3\rangle$.

(b) Show that when $X$ is applied to the left qubit of $|\omega_1\rangle$, we get $|\omega_3\rangle$.
(c) Show that when $\text{CNOT}_{01}$ is applied to $|\omega_2\rangle$, we get $|\omega_0\rangle$.
(d) Show that when $\text{CNOT} = \text{CNOT}_{10}$ is applied to $|\omega_3\rangle$, we get $|\omega_2\rangle$.

---

**Exercise 4.22.** The Mølmer-Sørensen (MS) gate is a two-qubit gate that can be naturally implemented on trapped ion quantum computers. It transforms $Z$-basis states by

$$|00\rangle \to \frac{1}{\sqrt{2}}(|00\rangle + i|11\rangle),$$
$$|01\rangle \to \frac{1}{\sqrt{2}}(|01\rangle - i|10\rangle),$$
$$|10\rangle \to \frac{1}{\sqrt{2}}(|10\rangle - i|01\rangle),$$
$$|11\rangle \to \frac{1}{\sqrt{2}}(|11\rangle + i|00\rangle).$$

(a) What is the MS gate as a matrix?
(b) Show that $\text{MS}^8 = I$. (You may use a computer.)

---

### *4.4.3 Toffoli Gate*

A three-qubit gate that often appears in quantum computing is the Toffoli gate, or controlled-controlled-NOT gate, that we discussed in Section 1.5.3. Since it is reversible, it is a quantum gate, and it flips the right qubit if the left and middle qubits are 1:

$$\begin{aligned}
\text{Toffoli}|000\rangle &= |000\rangle,\\
\text{Toffoli}|001\rangle &= |001\rangle,\\
\text{Toffoli}|010\rangle &= |010\rangle,\\
\text{Toffoli}|011\rangle &= |011\rangle,\\
\text{Toffoli}|100\rangle &= |100\rangle,\\
\text{Toffoli}|101\rangle &= |101\rangle,\\
\text{Toffoli}|110\rangle &= |111\rangle,\\
\text{Toffoli}|111\rangle &= |110\rangle.
\end{aligned}$$

Or

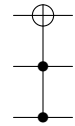
$$\text{Toffoli}|a\rangle|b\rangle|c\rangle = |a\rangle|b\rangle|ab \oplus c\rangle.$$

Recall from Section 1.5.3 that the Toffoli gate is universal for classical computing, and any efficient classical algorithm can be converted into an efficient algorithm only utilizing Toffoli gates. Since the Toffoli gate is a quantum gate, quantum computers can efficiently do everything a classical computer can efficiently do. In terms of complexity classes, P is contained within BQP.

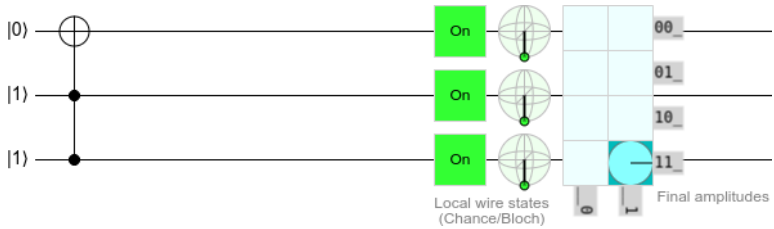
As a matrix, the columns correspond to Toffoli acting on $|000\rangle, |001\rangle, \ldots, |111\rangle$:

$$\text{Toffoli} = \begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{pmatrix}.$$

In Section 1.5.3, we drew the Toffoli gate as a box. In quantum computing, we typically draw the Toffoli gate similarly to the CNOT gate, with solid dots indicating the control qubits and $\oplus$ indicating the target:



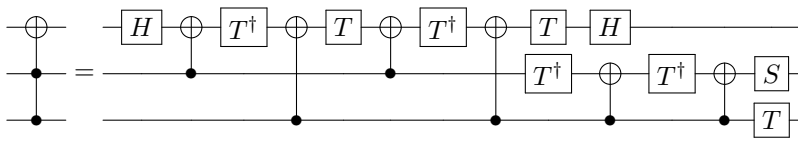
In Quirk, we simply drag two control dots onto the circuit, along with the $X$ gate:




We made the bottom two qubits both in the $|1\rangle$ state, so the Toffoli gate flips the top qubit to $|1\rangle$.

---

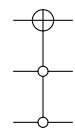
**Exercise 4.23.** Show that the Toffoli gate can be constructed from the one-qubit gates Hadamard $H$, phase $S$, $T$, and $T^\dagger$, plus the two-qubit CNOT gate:




Just do the matrix multiplications on the computer.

---

**Exercise 4.24.** Consider the anti-Toffoli gate, which was introduced in Exercise 1.41. In quantum computing, it is typically drawn like the anti-CNOT gate from Exercise 4.17, with open dots indicating the anti-controls:



(a) How does the anti-Toffoli gate act on each basis state?
(b) What is the anti-Toffoli gate as a matrix?

---

### 4.4.4 No-Cloning Theorem

Classically, it is easy to copy or *clone* information by reading each bit and writing it somewhere. In quantum computing, cloning qubits is more complicated. Say we have a qubit in some superposition state. If we measure it in the $Z$-basis, we get $|0\rangle$ or $|1\rangle$ with some probability. So, we do not learn the original superposition state. Furthermore, the measurement collapses the state to $|0\rangle$ or $|1\rangle$, meaning we lost whatever superposition state we originally had.

To investigate this in greater detail, say we have a qubit in a known quantum state, such as $|+\rangle$. Since we know its state, we can produce additional copies of it:

$$|+\rangle|0\rangle \xrightarrow{I\otimes H} |+\rangle|+\rangle.$$

We went from having one copy to two. So, copying a known quantum state is no problem.

The issue is copying an unknown quantum state. Say we have a qubit in an unknown quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, and we would like to make a copy of it:

$$|\psi\rangle|0\rangle \to |\psi\rangle|\psi\rangle.$$

Is there a quantum gate $U$ that allows us to copy or clone a general unknown qubit? $U$ would need to satisfy

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle.$$

Expressing this using linear algebra, we require

$$\begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} \\ U_{21} & U_{22} & U_{23} & U_{24} \\ U_{31} & U_{32} & U_{33} & U_{34} \\ U_{41} & U_{42} & U_{43} & U_{44} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} \\ U_{21} & U_{22} & U_{23} & U_{24} \\ U_{31} & U_{32} & U_{33} & U_{34} \\ U_{41} & U_{42} & U_{43} & U_{44} \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{pmatrix}$$

$$\begin{pmatrix} U_{11}\alpha + U_{13}\beta \\ U_{21}\alpha + U_{23}\beta \\ U_{31}\alpha + U_{33}\beta \\ U_{41}\alpha + U_{43}\beta \end{pmatrix} = \begin{pmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{pmatrix}$$

There are many possible solutions, such as

$$\begin{aligned} &U_{11} = \alpha, \quad U_{13} = 0, \quad U_{21} = 0, \quad U_{23} = \alpha, \\ &U_{31} = 0, \quad U_{33} = \alpha, \quad U_{41} = 0, \quad U_{43} = \beta, \end{aligned}$$

but this requires knowing $\alpha$ and $\beta$, which we do not know. Any general solution requires knowing $\alpha$ and $\beta$, so there is no operator $U$ that allows us to copy a general, unknown quantum state.

As another "proof," $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$ is akin to going from $\psi$ to $\psi^2$, and this is quadratic, not linear. The mathematics we are using is called linear algebra because matrices are linear. Vectors are transformed by linear transformations.

This result is called the *no-cloning theorem*. While classical information can be cloned, quantum information can not generally be cloned.

Using this theorem, some scientists have proposed quantum software that cannot be copied or pirated, and quantum money that cannot be copied or counterfeited, but that is beyond the scope of this textbook.

---

**Exercise 4.25.** Say there is a unitary $U$ that is able to clone qubits in two known states $|\psi\rangle$ and $|\phi\rangle$. That is,

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle,$$
$$U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle.$$

For example, an operator that can clone both $|0\rangle$ and $|1\rangle$ is CNOT, since $\text{CNOT}|00\rangle = |00\rangle$ and $\text{CNOT}|10\rangle = |11\rangle$. Taking the inner product of the previous two equations,

$$\begin{aligned}
\langle\psi|\langle 0|U^\dagger U|\phi\rangle|0\rangle &= (\langle\psi|\langle\psi|)\,(|\phi\rangle|\phi\rangle)\\
(\langle\psi|\langle 0|)\,(|\phi\rangle|0\rangle) &= (\langle\psi|\langle\psi|)\,(|\phi\rangle|\phi\rangle)\\
\langle\psi|\phi\rangle\langle 0|0\rangle &= \langle\psi|\phi\rangle\langle\psi|\phi\rangle\\
\langle\psi|\phi\rangle &= (\langle\psi|\phi\rangle)^2.
\end{aligned}$$

For $\langle\psi|\phi\rangle$ to be equal to its square, it must equal 0 or 1. Thus, $|\psi\rangle = |\phi\rangle$, or $|\psi\rangle$ and $|\phi\rangle$ are orthogonal. Thus, an operator can only clone states that are orthogonal.

Does there exist a quantum operator $U$ that can clone both

(a) $|+\rangle$ and $|-\rangle$?
(b) $|i\rangle$ and $|-i\rangle$?
(c) $|0\rangle$ and $|+\rangle$?

---

## 4.5 Quantum Adders

In Section 1.3, after defining classical bits and logic gates, we demonstrated how to compute something: the sum of two binary numbers, each of length $n$. Now that we have defined qubits and quantum gates, let us also construct quantum circuits that add binary numbers. Before we do that, however, let us review the classical ripple-carry adder.

### *4.5.1 Classical Adder*

First, to review, we can add two binary numbers as follows: